# COUNTY OF LOS ANGELES
# DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

JOHN NAIMO
AUDITOR-CONTROLLER


December 1, 2014

TO: Marvin Southard, D.S.W., Director
Department of Mental Health

FROM: John Naimo
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT COMPLIANCE REVIEW – RIO HONDO MENTAL HEALTH CENTER**

We have completed a review of the Department of Mental Health (DMH) Rio Hondo Mental Health Center's (RHMHC) compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic Clinical Health (HITECH) Act.[1] On October 6, 2014, we provided your Department with our final draft report, and conducted an exit conference on October 20, 2014. This report includes our findings, recommendations for corrective action, and your Department's response.

## Approach/Scope

Our review utilized the *HIPAA Privacy Rule and Health Information Technology for Economic Clinical Health (HITECH) Act Audit Tool* in evaluating RHMHC's compliance with the HIPAA Privacy Rule and DMH's HIPAA policies and procedures. DMH management is responsible for establishing and maintaining effective internal compliance with HIPAA regulations, and has oversight of the HIPAA program throughout their facilities. We considered DMH's internal controls over their compliance program, and the HIPAA Privacy Rule requirements that could have a direct and material effect on RHMHC.

Our review covered the Privacy Rule requirements for:

- Notice of Privacy Practice (NPP) for protected health information (PHI)
- Safeguards for PHI

[1] 45 Code of Federal Regulations (CFR) Parts 160 and 164

- Training
- Complaint process
- Refraining from intimidating or retaliatory acts
- Uses and disclosures requiring authorization
- Accounting for disclosures of PHI
- Minimum necessary standard
- HITECH Act Breach Notifications

## Results of Review and Recommendations

### Notice of Privacy Practices For Protected Health Information

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the NPP to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy.[2]

During our on-site review of RHMHC's main clinic and Bienestar Wellness Program (Bienestar), which is a program located at a separate location, we confirmed that the updated DMH NPP was displayed at the waiting rooms. In addition, we verified that hard copies of the NPP in English and Spanish were made available in the waiting rooms and on DMH's Internet website for patients to access without having to make a request.

We reviewed ten medical charts to verify the RHMHC management's statement that all patients are given the NPP on their first service delivery date, and noted that all the charts included the required acknowledgement of receipt.

Based on these findings, it appears that RHMHC is in compliance with the NPP standards.

### Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI. A covered entity must reasonably safeguard PHI and electronic PHI, and make reasonable efforts to prevent any intentional or unintentional use or disclosures that violate the Privacy Rule.

---

[2] Ibid., §164.520(c)

DMH Chief Information Office Bureau confirmed that all DMH workstations and laptop computers are equipped and protected with anti-malware/anti-virus software and port control software, which blocks downloading of PHI or other data to portable storage devices; and, the computers are configured to prevent workforce members from saving PHI onto their hard drives.

We verified that the fax machine, copier, and network printer were maintained in secure areas, and no PHI was left unattended on or near these office equipment items during our review. We also reviewed if proper safeguards were implemented in areas of medical records storage and workstations at the main clinic and *Bienestar*, and below are our findings.

***Main Clinic***

RHMHC management reported the main clinic's medical charts are stored in the lockable cabinets in a separate room, and only authorized workforce members and janitorial custodians, who arrive after business hours, have a key to the medical records room. RHMHC utilizes Accutrac, a records and information management software, to ensure medical records are properly tracked when distributed and returned. However, despite having a centralized system in place, RHMHC management reported to the Chief HIPAA Privacy Officer prior to this onsite audit that certain medical charts were missing due to check-in and filing errors. Although some charts were later returned by staff, the remaining missing charts needed to be recreated. Therefore, RHMHC management implemented a protocol to instruct medical records custodians to promptly account for all missing charts, and report incidents to DMH's Privacy Officer to determine whether or not certain incidents would constitute reportable breaches to the Office for Civil Rights (OCR). We reviewed the protocol and determined that the protocol is adequate.

***Bienestar***

Our on-site review of Bienestar noted several computer monitors and unlocked filing cabinets that store medical charts were in plain view and could be accessible by patients and visitors due to the layout and design of the workstations. We also noted a computer that displayed a calendar with sensitive patient information was left unattended in a workforce member's office with the door open, which may lead to incidental or prohibited disclosures of PHI.

Based on these findings, it appears that RHMHC failed to implement reasonable administrative and physical safeguards to fully safeguard PHI from wrongful disclosure.

**Recommendations**

**Rio Hondo Mental Health Center management:**

1. **Ensure that all inbound and outbound medical charts are properly tracked and returned to the medical records room (i.e., re-train all workforce members on the protocol for checking out a medical chart, perform monthly audits of medical records management, and report findings to the Department of Mental Health's Privacy Officer).**

2. **Ensure that the main clinic's medical records room is properly secured by restricting access to workforce members who have a business need (i.e., establish a schedule for the janitorial custodians to clean the medical records room when staff is present).**

3. **Evaluate the physical layout and design of Bienestar Wellness Program and implement reasonable physical safeguards to prevent incidental or prohibited disclosures of protected health information (i.e., install cubicle panels or other physical barriers around the workstations to shield the view of computer screens from the public).**

**Bienestar Wellness Program management:**

4. **Ensure the filing cabinets that store medical charts are properly secured (i.e., relocate the filing cabinets to a secured area or keep the cabinets locked at all times in the current location and restrict access to authorized workforce members).**

5. **Remind workforce members to take precautions to prevent unauthorized physical access to sensitive information from workstations (i.e., workstations not in use must be password protected or locked).**

## Training

RHMHC, as a HIPAA covered program, must train all members of its workforce on policies and procedures related to PHI as required by the HIPAA Privacy and Security Rules, as well as retraining staff when regulations are updated, to the extent necessary and appropriate for them to do their jobs. Workforce members include employees, volunteers, and trainees.

DMH Human Resources is responsible for ensuring its workforce members are trained on HIPAA compliance via the Learning Net. RHMHC management is responsible for training workforce members on DMH's HIPAA policies and procedures, and additional role-based training for their workforce members when applicable.

Our review of the training records showed that all workforce members have completed the required HIPAA training. RHMHC management attested that they also trained

workforce members on the DMH's HIPAA policies, which are placed in a binder and accessible via the Department's Intranet site. RHMHC is in compliance with the HIPAA training standards.

**Complaint Process**

A covered entity must provide a process for patients to complain about its policies and procedures. In addition, a covered entity must document all complaints received and their disposition, if any.

RHMHC management informed us that patient complaints are handled in accordance with DMH Policy Number 500.11, *HIPAA Privacy Complaints*, and RHMHC's internal protocols. Patients are directed to contact the Program Head, whose contact information is posted in the waiting area, or the Patients' Rights Office to file a complaint.

We observed that the DMH NPP posted in the waiting area informs patients that they may file a complaint with the U.S. Department of Health and Human Services (HHS), the County's Chief HIPAA Privacy Officer (CHPO), or the DMH Patients' Rights Office. We also verified that HIPAA complaint forms were available in the waiting area. We interviewed three randomly selected workforce members to test their knowledge about assisting patients who may wish to file a complaint, and their responses indicated that they are familiar with the complaint procedure. In the past year, no complaints were filed with the CHPO by RHMHC patients. It appears that the RHMHC complaint process complies with the complaints standard.

**Refraining from Intimidating or Retaliatory Acts**

Discussions with RHMHC management confirm they are aware of their obligation to comply with DMH Policy Number 500.18, *Refraining from Retaliatory or Intimidating Acts Against Individuals That Assert Rights Under HIPAA*. They also understand that OCR will investigate complaints against a covered entity that asserts retaliatory actions. In the past year, no complaints related to retaliatory or intimidating acts were filed with the CHPO by RHMHC patients. It appears that RHMHC is in compliance with the non-retaliation standard.

**Uses and Disclosures Requiring Authorization**

OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the patient. An authorization must specify a number of elements, including: (1) a description of the PHI to be used and disclosed, (2) the person authorized to make the use or disclosure, (3) the person to whom the covered entity may make the disclosure,

(4) an expiration date, and (5) the purpose for which the information may be used or disclosed.

RHMHC management reported that they follow DMH Policy Number 500.1, *Use and Disclosure of Protected Health Information Requiring Authorization.* Our review of the policy and the authorization form noted that they meet the Uses and Disclosures Requiring Authorization standard. Our review of the completed authorization forms from ten selected medical charts showed that the forms were properly filled out. It appears that RHMHC workforce members are trained and adhering to the uses and disclosures requiring authorization standard.

**Accounting for Disclosures of Protected Health Information**

The Privacy Rule gives patients the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, for up to six years after the disclosure. The following disclosures of PHI are excluded from the accounting requirement: (1) to the patient, (2) for treatment, (3) for payment and health care operations, (4) for facility directories, (5) pursuant to authorization, (6) pursuant to a limited data set agreement, (7) to persons involved in the patient's care, (8) for correctional institutions, and (9) for certain law enforcement purposes. In addition, an accounting of disclosures' log must be maintained in each patient's medical chart.

RHMHC management reported that they follow DMH Policy Number 500.6, *Accounting of Disclosures of Protected Health Information,* to track all non-routine disclosures. However, our review of four completed accounting of disclosures logs, provided by RHMHC management, noted that workforce members did not appear to have a clear understanding of the information that should be tracked. Specifically, staff documented disclosures of PHI for treatment purposes, with patients' authorizations, and when patients provided information to them. We provided additional guidance to DMH's Privacy Officer to ensure that RHMHC managers and employees are properly documenting the disclosures of PHI per the regulations.

**Recommendations**

6. **Department of Mental Health Privacy Officer provide guidance to Rio Hondo Mental Health Center management on the Accounting of Disclosures of Protected Health Information standard.**

7. **Rio Hondo Mental Health Center management ensure that workforce members are re-trained on the Department of Mental Health Policy Number 500.6, Accounting of Disclosures of Protected Health Information.**

## Minimum Necessary Rule

When using, disclosing, or requesting PHI from another covered entity, the Privacy Rule requires a covered entity to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. OCR provides covered entities with flexibility to address their unique circumstances, and make their own assessment of what PHI is necessary for a particular purpose. Discussions with RHMHC management indicate that workforce members are aware of the minimum necessary standard.

## HITECH Act Breach Notification

HHS issued regulations requiring health care providers to notify patients when their health information is breached. Specifically, health care providers and other covered entities must promptly notify affected patients of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 patients. Breaches affecting fewer than 500 patients will be reported to the HHS Secretary annually. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate. Further, HHS' Breach Notification regulations emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured PHI.

RHMHC management informed us that the workforce members are aware that they must report all incidents involving suspected or actual breaches to their immediate supervisors, who will report to the DMH Privacy Officer. We reviewed DMH Policy Number 500.28, *Responding to Breach of Protected Health Information,* and it shows clear guidelines to workforce members in the event a breach or suspected breach of PHI is discovered. We also noted the facility implemented an internal protocol regarding how to respond to a breach and trained workforce members accordingly.

## Conclusion

We discussed our findings with DMH and RHMHC management on October 20, 2014. Their attached response indicates that they agree with our recommendations and have already taken corrective actions to implement the majority of our findings and recommendations. The DMH Privacy Officer will work with RHMHC management to ensure that all of our recommendations are implemented. We will follow up with RHMHC management in 120 days from the date of this report to ensure all deficiencies have been corrected. We thank DMH's Privacy Officer and RHMHC managers and staff for their cooperation and assistance during this review.

Please call me if you have any questions, or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166.

JN:RGC:GZ:LTM:JC

Attachment

c: Brence Culp, Acting Chief Executive Officer
Mark J. Saladino, County Counsel
Stephanie Jo Reagan, Principal Deputy County Counsel, County Counsel
Robert Pittman, Chief Information Security Officer, Chief Information Office
Judith Weigand, Compliance Officer, Department of Mental Health
Ginger Fong, Privacy Officer, Department of Mental Health
Audit Committee
Health Deputies

LAC DMH
LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH
550 S. VERMONT AVE., LOS ANGELES, CA 90020 HTTP://DMH.LACOUNTY.GOV

MARVIN J. SOUTHARD, D.S.W.
Director
ROBIN KAY, Ph.D
Chief Deputy Director
RODERICK SHANER, M.D.
Medical Director

October 21, 2014

To: Julia Chen, MA
Assistant HIPAA Privacy Officer
Los Angeles County, Department of Auditor-Controller

From: Ginger Fong
Privacy Officer, Compliance Program
Los Angeles County, Department of Mental Health (LAC-DMH)

Subject: HIPAA and HITECH Act Compliance Review
Rio Hondo Mental Health Center (RHMHC)

This is our response to the Auditor-Controller's Draft report concerning compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) at Rio Hondo Mental Health Center (RHMHC).

**Auditor-Controller Recommendation #1:**

Ensure that all inbound and outbound medical charts are properly tracked and returned to the medical records room (i.e., retrain all workforce members on the protocol for checking out a medical chart, perform periodic audits of medical records management, and report findings to DMH Privacy Officer).

**RHMHC Response:**

RHMHC agrees with the Auditor-Controller's recommendation.

A protocol has been established and distributed to all staff and have been trained for the proper monitoring and tracking of client medical charts. Staffs are required to request charts in writing from the designated medical records staff, which pull the chart and register to whom it was given in the Accutrack system. At the end of the day, or before, the person receiving the chart is expected to return the chart to the medical records staff, who will register the receipt of the chart in the Accutrack system. On the next business day, any charts that were not returned to medical records the previous day are reported to the clinic staff assistant and Program Head. A search for the record is immediately conducted, and if the chart cannot be located, the missing chart is reported to the DMH Privacy Officer by the Program Head. In addition, the Program Head will perform periodic audits of medical records tracking on a monthly basis, reviewing all charts pulled on the previous month to assure compliance with the tracking procedure.

**Auditor-Controller Recommendation #2:**

Ensure that the main clinic's medical records room is properly secured by restricting access to workforce members who have a business need (i.e., establish a schedule for the janitorial custodians to clean the medical records room when staff is present).

**RHMHC Response:**

While we agree with the Auditor's recommendation, however we are unable to meet it as the janitorial staff is only available after hours in the evening.

Therefore, a procedure has been establish to assure that access to the medical records is restricted to designated medical records staff, approved volunteers, and their supervisor, the Staff Assistant. The janitorial service for medical records is provided on Wednesday evenings. At the close of business, all medical records are secured and locked in the chart shelves, and the medical records office is left open for the janitorial staff to clean. When they are finished they leave the office locked.

**Auditor-Controller Recommendation #3:**

Evaluate the physical layout and design of Bienestar Wellness Program and implement reasonable physical safeguards to prevent incidental or prohibited disclosures of protected health information (i.e., install cubicle panels or other physical barriers around the workstations to shield the view of computer screens from the public).

**RHMHC Response:**

We agree with the Auditor's recommendation.

Auditor stated that it was reported by Bienestar management that clients are escorted through the door next to the receptionist by the clinician to the group room or individual office after they have checked in. In doing so, the client goes through an area that has desks, computers, and medical files in the cabinets with no barriers around them. Bienestar management stated that currently, clients can enter the clinic only through the group room or the staff workstation area.

In response to the recommendation, Bienestar will no longer allow access to clients in the area designated for workstations and Medical Records files as it is an office area restricted to staff only. Clients shall enter the treatment rooms through the entrance on the left, which is also the entrance to the group room. If that is not possible because a group is in progress, clients will check in with the receptionist, then enter the offices through a second doorway in the hall, which is normally kept locked but which can be opened by the clinicians from the inside of the suite. Staff only will enter the offices through the right, which leads to the workstations. As there will be no client or visitor

traffic through the workstation area, there should be no danger of incidental disclosures. The program lead and all staff have been reminded to utilize this procedure at all times.

**Bienestar Wellness Program Management:**

**Auditor-Controller Recommendation #4:**

Ensure the filing cabinets that store medical charts are properly secured (i.e., relocate the filing cabinets to a secured area or keep the cabinets locked at all times in the current location and restrict access to authorized workforce members).

**RHMHC Response:**

We agree with the Auditor's recommendation.

Access to the area where the filing cabinets are located is restricted to authorized workforce members only. In addition, a protocol has been established to assure only designated staff have access to the records, and that the cabinets securing said records are locked at all times, unless we are pulling or returning charts.

**Auditor-Controller Recommendation #5:**

Remind workforce members to take precautions to prevent unauthorized physical access to sensitive information from workstations (i.e., workstations not in use must be password protected or locked).

**RHMHC Response:**

We agree with the Auditor's recommendation.

Workforce members have been instructed to take precautions to prevent unauthorized physical access to sensitive information from workstations. All client information must be secured in a desk drawer when a client is in the office, and computers must be locked, with the exception of information related to the client being seen in the office with the provider of service. When a provider is not at their desk, all client related information must be secured and the computers locked to prevent accidental breaches of confidentiality

**Auditor-Controller Recommendation #6:**

Department of Mental Health Privacy Officer provides guidance to Rio Hondo Mental Health Center management on the Accounting of Disclosures of Protected Health Information standard.

**RHMHC Response:**

We agree with the Auditor's recommendation.

The DMH Privacy Officer is scheduled to re-train the management staff at Rio Hondo on Policy No. 500.6, Accounting of Disclosures of Protected Health Information, in early November.

Management staff will subsequently train all staff under their supervision at the next all staff meeting on November 19, 2014. In addition, the DMH Privacy Officer will provide guidance and be available to respond to questions and concerns regarding the Accounting of Disclosures policy and procedures

On an as needed basis.

**Auditor-Controller Recommendation #7:**

Rio Hondo Mental Health Center management ensures that workforce members are re-trained on the Department of Mental Health policy 500.6, Accounting of Disclosures of Protected Health Information.

**RHMHC Response:**

We agree with the Auditor's recommendation.

As mentioned above, the DMH Privacy Officer is scheduled to re-train the supervisory staff and they will subsequently train all staff under their supervision. In addition, review of the Accounting of Disclosure Form will become a part of our QA procedure.